|  |  |
| --- | --- |
|  | **ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ**  ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ  Τομέας Επικοινωνιών, Ηλεκτρονικής & Συστημάτων Πληροφορικής  Εργαστήριο Διαχείρισης και Βέλτιστου Σχεδιασμού Δικτύων - NETMODE  Ηρώων Πολυτεχνείου 9, Ζωγράφου, 157 80 Αθήνα, Τηλ: 210-772.2503, Fax: 210-772.1452  e-mail: maglaris@netmode.ntua.gr, URL: http://www.netmode.ntua.gr |

Επαναληπτική Εξέταση στο Μάθημα:

"ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ - ΕΥΦΥΗ ΔΙΚΤΥΑ"

(9ο Εξάμηνο)

Διδάσκων: Β. Μάγκλαρης

**17/02/2017**

Ανοικτά Βιβλία & Σημειώσεις. Διάρκεια **2.5 ώρες**.

Θυμίζουμε ότι οι εργαστηριακές ασκήσεις ήταν υποχρεωτικές και αποτελούν το **30%** της συνολικής βαθμολογίας. **ΚΑΛΗ ΕΠΙΤΥΧΙΑ!**

Οι βαθμοί θα ανακοινωθούν στο URL: **http://www.netmode.ntua.gr**

**ΘΕΜΑ 1 (4 μονάδες)**

Δίνεται το τοπικό δίκτυο του σχήματος, με πρόθεμα (prefix) διευθύνσεων 83.212.0.0/16, το οποίο αποτελείται από τρία διασυνδεόμενα υποδίκτυα.



Τα υποδίκτυα *I*, *II* συνδέονται πάνω στον ίδιο μεταγωγέα (Ethernet Switch) σαν δύο διαφορετικά VLAN, ένα για κάθε υποδίκτυο. Η πρόσβαση στο Internet για τα δίκτυα αυτά γίνεται μέσω του δρομολογητή (Router) 1 και του δρομολογητή (Router) του ISP 1 με IP 62.217.118.62/30. Το υποδίκτυο *ΙΙΙ* έχει πρόσβαση στο Internet μέσω του δρομολογητή (Router) 2 και του δρομολογητή (Router) του ISP 2 με IP 62.217.100.38/30.

Α. Ζητείται να προσδιοριστούν τα παρακάτω 4 υποδίκτυα (subnets) με την μέγιστη οικονομία διευθύνσεων:

1. Το υποδίκτυο *I* που περιλαμβάνει συνολικά 61 υπολογιστές. Ο υπολογιστής Α έχει IP 83.212.111.137.
2. Το υποδίκτυο *II* που περιλαμβάνει συνολικά 13 υπολογιστές. Ο υπολογιστής Β έχει IP 83.212.112.35.
3. Το υποδίκτυο *III* που περιλαμβάνει συνολικά 7 υπολογιστές. Ο υπολογιστής C έχει IP 83.212.113.88.
4. Το υποδίκτυο για τη σύνδεση των δρομολογητών 1, 2 (interfaces 1b, 2b). Η IP του interface 2b είναι 83.212.114.5.

Σημείωση: Η διαχειριστική IP του μεταγωγέα ανήκει στο πεδίο IP του υποδικτύου *IΙ*

Β. Αποδώστε IP διευθύνσεις στα interfaces 1a, 1b, 1c, 2a, 2c, των δρομολογητών 1 και 2. Περιγράψτε τους πίνακες δρομολόγησης του δρομολογητή 1 και των υπολογιστών B και C για όλα τα υποδίκτυα και το Internet στη μορφή:

|  |  |  |
| --- | --- | --- |
| Destination | Netmask | Gateway |

Γ. Τι διαχειριστικές αλλαγές απαιτούνται ώστε να υπάρχει η δυνατότητα υπολογιστών που ανήκουν στα υποδίκτυα *Ι*, *ΙΙ* να έχουν εναλλακτική δρομολόγηση από και προς το Internet μέσω του ISP 2; Τι απαιτείται ώστε να υπάρχει η δυνατότητα υπολογιστών που ανήκουν στο υποδίκτυο *ΙΙΙ* να έχουν εναλλακτική δρομολόγηση από και προς το Internet μέσω του ISP 1;

Δ. Δείξτε τα αποτελέσματα από την εκτέλεση των εντολών traceroute: (i) από τον υπολογιστή B προς τον κόμβο www.grnet.gr (62.217.124.68) και (ii) από τον υπολογιστή C προς τον κόμβο www.grnet.gr (62.217.124.68). Επίσης (iii) από τον υπολογιστή C προς τον υπολογιστή A.

(iv) Έστω ότι η σύνδεση μεταξύ των δρομολογητών 1 και 2 τίθεται προσωρινά εκτός λειτουργίας. Ποιο είναι το αποτέλεσμα της εντολής traceroute από τον υπολογιστή C προς τον υπολογιστή Α.

Σημείωση: Οι διευθύνσεις IP στις απαντήσεις δεν θα αφορούν hops στο εσωτερικό του ISP και το γενικότερο Internet.

Ε. Ποια διεύθυνση MAC προορισμού πρέπει να έχουν πακέτα που στέλνονται από τον υπολογιστή A: (1) Προς τον υπολογιστή B; (2) Προς τον υπολογιστή C; (3) Προς τον υπολογιστή D (όπου D τυχαίος υπολογιστής στο υποδίκτυο *I* );

ΣΤ. Έστω πως ο υπολογιστής A στέλνει ένα ARP ερώτημα για να μάθει την διεύθυνση MAC του interface 1a του δρομολογητή 1. Θα φτάσει αυτό το ερώτημα σε κόμβο εκτός του υποδικτύου *I*; Αλλάζει κάτι στην υποθετική περίπτωση που το Ethernet Switch **δεν** υποστηρίζει VLANs; Τεκμηριώστε τις απαντήσεις σας.

**ΘΕΜΑ 2 (3 μονάδες)**

Παρακάτω είναι τυπωμένα DNS (Domain Name System) Resource Records για το οποία έχει ερωτηθεί και έχει απαντήσει ο κόμβος dolly.netmode.ece.ntua.gr.

grnet.gr. 1807 IN NS ns0.grnet.gr.  
averel.netmode.ntua.gr 86400 IN A 147.102.13.1  
ns1.grnet.gr. 13339 IN A 83.212.5.22  
ns1.grnet.gr. 20602 IN AAAA 2001:648:2ffc:112::2  
telecom.ntua.gr. 75414 IN NS ulysses.noc.ntua.gr.  
ntua.gr. 86400 IN MX 20 achilles.noc.ntua.gr.  
ntua.gr. 86400 IN MX 20 diomedes.noc.ntua.gr.  
ntua.gr. 86400 IN MX 20 ulysses.noc.ntua.gr.  
www.netmode.ntua.gr. 86400 IN CNAME dolly.netmode.ece.ntua.gr.  
patroklos.noc.ntua.gr. 36154 IN A 147.102.222.211

mail.netmode.ntua.gr. 86400 IN CNAME dolly.netmode.ece.ntua.gr.  
f.root-servers.net. 478953 IN A 192.5.5.241  
c.root-servers.net. 421734 IN A 192.33.4.12  
ftp.ntua.gr. 23875 IN CNAME patroklos.noc.ntua.gr  
ftp.netmode.ntua.gr. 86400 IN CNAME dolly.netmode.ntua.gr

A) Ζητείται να ερμηνεύσετε τι είδους πληροφορίες περιέχονται στις διάφορες στήλες σχετικά με κάθε μία από τις εγγραφές.

B) Ο web server του εργαστηρίου NETMODE σε ποιο κόμβο πιστεύετε ότι φιλοξενείται; Τι άλλη υπηρεσία πιστεύετε ότι προσφέρεται από αυτό τον κόμβο;

Γ) Γιατί έχει ο *f.root-servers.net* και ο *c.root-servers.net* στην 2η στήλη μεγάλη τιμή;

Δ) Μετά από κάποιο χρονικό διάστημα τα ίδια queries θα έχουν τα εξής αποτελέσματα:

grnet.gr. 1707 IN NS ns0.grnet.gr.  
averel.netmode.ntua.gr 86400 IN A 147.102.13.1  
ns1.grnet.gr. 13239 IN A 83.212.5.22  
ns1.grnet.gr. 20502 IN AAAA 2001:648:2ffc:112::2  
telecom.ntua.gr. 75314 IN NS ulysses.noc.ntua.gr.  
ntua.gr. 86300 IN MX 20 achilles.noc.ntua.gr.  
ntua.gr. 86300 IN MX 20 diomedes.noc.ntua.gr.  
ntua.gr. 86300 IN MX 20 ulysses.noc.ntua.gr.  
www.netmode.ntua.gr. 86400 IN CNAME dolly.netmode.ece.ntua.gr.  
patroklos.noc.ntua.gr. 36054 IN A 147.102.222.211  
mail.netmode.ntua.gr. 86400 IN CNAME dolly.netmode.ece.ntua.gr.

f.root-servers.net. 478853 IN A 192.5.5.241  
c.root-servers.net. 421634 IN A 192.33.4.12  
ftp.ntua.gr. 23775 IN CNAME patroklos.noc.ntua.gr  
ftp.netmode.ntua.gr. 86400 IN CNAME dolly.netmode.ntua.gr

Με βάση τις παραπάνω πληροφορίες για ποιες από τις παραπάνω πληροφορίες πιστεύετε ότι ο DNS server dolly.netmode.ntua.gr είναι ο καθ’ ύλην αρμόδιος (Authoritative);

E) Ο κόμβος dolly.netmode.ntua.gr ανήκει στο υποδίκτυο 147.102.13.0/24 του σχήματος. Η σύνδεση του υποδικτύου με το διαδίκτυο γίνεται μέσω του δρομολογητή (Router) 1 με interfaces a, και b. Το interface (a) έχει MAC address 74:a0:2f:0c:d9:ff και IP address 147.102.13.200.

Ο κόμβος dolly.netmode.ntua.gr (διεύθυνση MAC 00:1d:09:05:33:c7 και IP 147.102.13.10) δέχεται μεγάλο όγκο πακέτων που είναι μέρος μιας κατανεμημένης επίθεσης Άρνησης Παροχής Υπηρεσίας (Distributed Denial of Service – DDoS). Η επίθεση βασίζεται στο πρωτόκολλο DNS (όχι AXFR Queries). Ανάμεσα στους επιτιθέμενους είναι οι εξής IP διευθύνσεις: 191.96.249.38, 113.106.83.120, 185.159.36.10.



Ανάμεσα στον δρομολογητή (Router) 1 και στον κόμβο dolly υπάρχει μεταγωγέας με λειτουργικότητα OpenFlow και τοπικές πόρτες 1 και 2.

1. Αναφέρατε τρόπους προστασίας του δικτύου 147.102.13.0/24 από την επίθεση, χρησιμοποιώντας δυνατότητες/λειτουργικότητα του δρομολογητή.
2. Περιγράψτε τους κανόνες OpenFlow (με όσο το δυνατόν περισσότερα πεδία) που πρέπει να τοποθετηθούν στον μεταγωγέα ώστε:
3. Η φυσιολογική κίνηση να προωθείται κανονικά.
4. Η κακόβουλη κίνηση να απορρίπτεται.

Οι κανόνες πρέπει να είναι στην μορφή:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| In port | MAC src | MAC dst | Ether type | VLAN PCP | VLAN ID | IP src | IP dst | IP protocol | IP ToS | Port src | Port dst | Priority | Action |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Πιθανές χρήσιμες πληροφορίες:

Ether Type: 0x0800 (IPv4), 0x0806 (ARP), 0x88CC (Link Layer Discovery Protocol)

IP Protocol number: 1 (ICMP), 6 (TCP), 17 (UDP)